IN THE UNITED STATES DISTRICT COURT FOR

THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**Criminal No. 15-1**
DMITRIJ HARDER	**:**	

ORDER

AND NOW, this ____ day of _____ 2016, upon consideration of the defendant's motion to suppress, and the government's response thereto, and following a hearing on the matter, it is ORDERED that the defendant's motion is DENIED.

BY THE COURT:

_____
HONORABLE PAUL S. DIAMOND
United States District Court Judge

IN THE UNITED STATES DISTRICT COURT FOR

THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	**:**	
v.	**:**	**Criminal No. 15-1**
DMITRIJ HARDER	**:**	

GOVERNMENT'S RESPONSE IN OPPOSITION TO DEFENDANT DMITRIJ HARDER'S MOTION TO SUPPRESS EMAILS OBTAINED FROM GOOGLE AND 1&1 INTERNET

The United States of America, by and through Zane David Memeger, United States Attorney for the Eastern District of Pennsylvania, Michelle L. Morgan, Assistant United States Attorney for the District, and Andrew Weissmann, Chief, and Jason D. Linder, Senior Trial Attorney, U.S. Department of Justice, Criminal Division, Fraud Section, hereby responds to the defendant's motion to suppress electronic evidence seized during the execution of two search warrants issued on October 15, 2010: the first, a warrant to search information associated with the e-mail account "dharder@chestnut-consulting.com" (the "Chestnut Email Account") from Internet service provider 1&1 Internet Inc. ("1&1 Internet"), and the second, a warrant to search information associated with the email accounts "dmitri.harder@gmail.com" (the "Gmail Email Account") and "aryjenko@googlemail.com" from Internet service provider Google Inc. ("Google") (collectively, the "Email Search Warrants"). Contrary to the defendant's assertions, these warrants and their execution fully complied with the requirements of the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure. Accordingly, the motion should be denied.

FACTUAL BACKGROUND

On October 15, 2010, Magistrate Judge L. Felipe Restrepo issued the Email Search Warrants. The applications for the warrants incorporated an affidavit from FBI Special Agent Stephen R. Gray (the "Gray Affidavit") setting forth the probable cause supporting the warrants. As described in the Gray Affidavit, the Federal Bureau of Investigation ("FBI") and the United States Department of Justice ("DOJ") commenced a criminal investigation in February 2010 into the potentially corrupt conduct of the defendant; Andrey Ryjenko, a banker at the European Bank for Reconstruction and Development ("EBRD"); and Tatjana Sanderson, Ryjenko's sister. (Gray Aff. ¶¶ 6, 8.)

The Gray Affidavit included detailed allegations establishing probable cause that the corrupt conduct had occurred and that it constituted violations of federal law, including the Foreign Corrupt Practices Act of 1977 ("FCPA"), as amended, 15 U.S.C. § 78dd-1 et seq.; 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1957 (money laundering); 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1001 (false statements); and 31 U.S.C. § 5314 (FBAR). (Gray Aff. ¶ 5.) The allegations in the Gray Affidavit recounted information from witness statements, bank records, emails, and other documents showing the defendant's corrupt multimillion dollar payments to Sanderson in connection with projects over which her brother Ryjenko had authority and the steps the defendant and Sanderson took to conceal the true nature and purpose of those payments. (Id. ¶¶ 6-58.) The evidence recited in the Gray Affidavit included a description of false exculpatory statements the defendant made during an interview at John F. Kennedy International Airport ("JFK") on February 26, 2010. (Id. ¶¶ 10, 13, 14, 58.)

The Gray Affidavit also established probable cause that evidence of these crimes would be found in the Chestnut Email Account and the Gmail Email Account. The affidavit detailed

communications in furtherance of the corrupt scheme between the Chestnut Email Account and (a) Ryjenko (id. ¶¶ 62, 63, 70), (b) other EBRD employees in connection with the Vostok and Azmeco transactions (id. ¶¶ 52, 72), and (c) Sanderson (id. ¶¶ 24, 28, 44-48, 53, 60). Similarly, the affidavit described the communications between the Gmail Email Account and Ryjenko. (Id. ¶¶ 65, 66.) The defendant, in his capacity as Chestnut Consulting Group's custodian of records, had previously produced to the government some of the emails from the Chestnut Email Account recounted in the Gray Affidavit. (Id. ¶¶ 24, 28, 44, 60.) He had produced these emails in response to subpoenas served on him at the end of his February 26, 2010, interview. (Id. ¶¶ 28, 53.) The Gray Affidavit also recounted communications from the Chestnut Email Account that the EBRD and the City of London Police had gathered during their investigations and that evidenced the defendant's corrupt scheme. (Id. ¶¶ 44, 52, 62, 63, 70.)

Based on the probable cause detailed in the Gray Affidavit, Judge Restrepo issued the Email Search Warrants, which authorized agents to search the Chestnut Email Account and the Gmail Email Account. (Br. Attach. A. at 37, Attach. B. at 37.) The Email Search Warrants permitted agents to seize only documents that met three criteria. First, a document had to "constitute[] fruits, evidence and instrumentalities of violations of 15 U.S.C. § 78dd-1 et seq. (Foreign Corrupt Practices Act), 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1957 (Money Laundering), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 1001 (False Statements), and 31 U.S.C. § 5314 (FBAR)." (Br. Attach. A. at 38-39, Attach. B. at 38-39.) Second, the warrant permitted seizure of such documents only if they "involv[ed] Dmitrij Harder, Andrey Ryjenko, Tatjana Sanderson ("Subjects") since February 1, 2007 . . . ." (Br. Attach. A. at 39, Attach. B. at 39.) And third, the documents had to contain "information pertaining to the following matters":

a. Communications Between the Subjects [the defendant, Ryjenko, and Sanderson];

b. Communications between the Subjects and employees of Chestnut Consulting Group, Inc. or Dmitrij Harder;

c. Communications between the Subjects and employees of the European Bank for Reconstruction and Development;

d. Communications between the Subjects and officers, employees, or agents of the following companies: (1) Irkutsk Oil and Gas, (2) Hawkley Oil and Gas, (3) Azerbaijan Methanol Company, (4) Vostok Energy Limited, and (5) Itera International Group;

e. Communications between the Subjects and financial institutions at which the Subjects banked during the course of the scheme;

f. Communications relating to payments to or from the Subjects to facilitate the scheme; and

g. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

(Br. Attach. A. at 38-39, Attach. B. at 38-39.)

The FBI served the Email Search Warrants on Google and 1&1 Internet on October 15, 2010, and October 18, 2010, respectively. Both Internet service providers produced documents to the FBI in response to the warrants within two weeks.[1] Beginning in February 2011, the FBI conducted targeted searches for documents that were on or near dates relevant to the transactions under investigation and between individuals who were subjects of the investigation. Many of the documents produced in response to the Email Search Warrants were in Russian and have not yet been translated. The government has produced all of the returns from the Email Search Warrants to the defendant.

[1] On October 28, 2010, the FBI shared the search warrant returns to the City of London Police. Shortly afterward, a City of London Police detective told the FBI that he had seen the header of an email between Ryjenko and his attorney and then stopped reading. In response, on December 14, 2010, the FBI submitted a request to a computer forensics laboratory to segregate potentially privileged emails for both Harder and Ryjenko. The lab returned non-privileged emails to the FBI on February 23, 2011. The government has established a filter team led by a Department of Justice attorney to review the potentially privileged emails segregated out by the computer lab.

ARGUMENT

The defendant's motion should be denied because the Email Search Warrants fully complied with the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure. The warrants satisfied the Fourth Amendment because they were not overbroad, described the items to be seized with particularity, amply established probable cause, and were executed in a reasonable manner. The warrants complied with Rule 41 because 18 U.S.C. § 2703(a) authorized the magistrate judge to issue the warrants as to out-of-state Internet service providers, and because the government provided notice to the Internet service providers from whose premises the property was taken.

I. The Defendant Lacks Standing to Seek Suppression of Ryjenko's Emails

As a threshold matter, the defendant does not have standing to request suppression of Andrey Ryjenko's Google emails. The defendant's proposed order seeks as a remedy "that all emails obtained by the government by search warrants to Google Inc. and 1&1 Internet Inc. shall be SUPPRESSED." (Doc. No. 79.) That order would include not only the defendant's two email accounts, but also Ryjenko's. Fourth Amendment rights, though, are personal. See Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) ("Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." (citation and internal quotation marks omitted)); United States v. Stearn, 597 F.3d 540, 551 (3d Cir. 2010) ("To invoke the Fourth Amendment's exclusionary rule, a defendant must demonstrate that his own Fourth Amendment rights were violated by the challenged search or seizure." (citation omitted)). The defendant would "bear[] the burden of proving . . . that he had a legitimate expectation of privacy" in Ryjenko's email account. Rawlings v. Kentucky, 448 U.S. 98, 104 (1980). Because the defendant did not attempt—and could not make—such a showing, he lacks standing to seek

suppression of Ryjenko's emails. Accordingly, the government responds below to the defendant's arguments only as they apply to his own email accounts.

II. The Email Search Warrants Complied with the Fourth Amendment

A. The Email Search Warrants Were Sufficiently Particular

The Email Search Warrants complied with the Fourth Amendment requirement that they "particularly describ[e] the place to be searched and the persons or things to be seized." U.S. Const. amend. IV. The scope of the particularity clause is limited to "two matters . . . the place to be searched and the persons or things to be seized." United States v. Grubbs, 547 U.S. 90, 97 (2006) (internal quotation marks omitted). This requirement guards against the issuance of warrants that "essentially authorize 'a general exploratory rummaging in a person's belongings.'" United States v. Yusuf, 461 F.3d 374, 393 (3d Cir. 2006) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971)). "A warrant is not general unless it can be said to 'vest the executing officer with unbridled discretion to conduct an exploratory rummaging through [defendant's] papers in search of criminal evidence.'" United States v. Leveto, 540 F.3d 200, 211 (3d Cir. 2008) (alteration in original) (quoting United States v. Christine, 687 F.2d 749, 753 (3d Cir. 1982)).

Thus, although courts have never required precise specification of every item to be seized, they do require that a warrant reasonably cabin the discretion of those charged with executing it. See, e.g., Yusuf, 461 F.3d at 395 ("[T]he breadth of items to be searched depends upon the particular factual context of each case and also the information available to the investigating agent that could limit the search at the time the warrant application is given to the magistrate."); Christine, 687 F.2d at 760 ("the use of generic classifications in a warrant is acceptable when a more precise description is not feasible"); United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000) ("A warrant must be sufficiently specific to permit the rational exercise of

judgment [by the executing officers] in selecting what items to seize."); United States v. American Investors of Pittsburgh, 879 F.2d 1087, 1105-06 (3d Cir. 1989) ("The fact that the warrant authorized a search for a large amount of documents and records does not necessarily render the search invalid so long as there exists a sufficient nexus between the evidence to be seized and the alleged offenses."). A warrant is not sufficiently particularized if it authorizes "the seizure of 'evidence' without mentioning a particular crime or criminal activity to which the evidence must relate." United States v. George, 975 F.2d 72, 77 (2d Cir. 1992) (citation omitted).

Here, the Email Search Warrants fully satisfied the particularity requirement. The Attachment A to each warrant specifies the places to be searched and is limited to information associated with three specifically identified email accounts. (Br. Attach. A. at 37, Attach. B. at 37.) The Attachment B to each warrant identifies with particularity the items to be seized, which are limited to electronic data that "constitutes fruits, evidence, and instrumentalities" of FCPA and other specified violations. (Br. Attach. A. at 38-39, Attach. B. at 38-39.) The items to be seized, further, must "involv[e] Dmitrij Harder, Andrey Ryjenko, Tatjana Sanderson ("Subjects") since February 1, 2007." (Br. Attach. A. at 39, Attach. B. at 39.) That date limitation on the items the government may seize under the Email Search Warrants belies the defendant's assertion that there "was no date limitation" in the Email Search Warrants. (Br. at 16.) The items to be seized were further limited to seven specific categories of documents. (Br. Attach. A. at 39, Attach. B. at 39.)

The Email Search Warrants appropriately constrained agents because they were authorized only to search the places specified in the Attachment As for the items specified in the Attachment Bs that related to specific crimes and subjects, and within the specific dates, recited

in the Attachment Bs. The warrants did not remotely resemble a general warrant and, in fact, are far more specific and particularized than many other warrants courts have upheld. See, e.g., Yusuf, 461 F.3d at 395 (warrant seeking broad categories of business records from company allegedly involved in complex money laundering scheme satisfied particularity clause where warrants referred to several specifically enumerated crimes, sought records for specific years, and limited search to a select group of entities and individuals); United States v. Kuc, 737 F.3d 129, 132-33 (1st Cir. 2013) (same); United States v. Adjani, 452 F.3d 1140, 1148-49 (9th Cir. 2006) (same); United States v. Fattah, Case No. 14-cr-409, 2015 WL 289983, at *4-5 (E.D. Pa. Jan. 22, 2015) (holding that warrant in a complex case satisfied the particularity requirement even though it sought seven years' worth of documents described only in very broad categories such as "[a]ll financial records" and "[a]ll records of money and any other assets sent abroad" and "electronic equipment used to store the information") (alterations in original). Accordingly, the Email Search Warrants were sufficiently particular to satisfy the Fourth Amendment.

B. The Email Search Warrants Were Not Overbroad

The Email Search Warrants also were not overbroad. The defendant's main arguments to the contrary seem to be that the warrants demanded "production of all email communications" and that "[t]here was no date limitation on the warrant as to what the government was able to obtain . . . ." (Br. at 16 (emphasis omitted).) The defendant cites no authority to support his contention that those are bases for the Court to find the Email Search Warrants were overbroad.

In fact, as the Third Circuit has explained, the initial review of both relevant and non-relevant material is necessary in complex criminal cases where the government must pore over large numbers of documents to find evidence of the crime:

> [I]n searches for papers, it is certain that some innocuous documents will be at least cursorily perused in order to determine whether they are among those papers to be seized. But no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the terms of the warrant. This flexibility is especially appropriate in cases involving complex schemes spanning many years that can be uncovered only by extracting scrutiny of intricate financial records.

Christine, 687 F.2d at 760 (citations omitted); see also Andresen v. Maryland, 427 U.S. 463, 480 n.10 (1976) ("The complexity of an illegal scheme may not be used as a shield to avoid detection when the State has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession.").

The reasoning of Andresen and Christine is particularly instructive where criminal schemes involve electronic communication and devices. Indeed, "[i]n the context of suppression motions, courts have routinely upheld the seizure or copying of hard drives and other storage devices in order to effectuate a proper search for the categories of documents or files listed in a warrant." In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386, 393 (S.D.N.Y. 2014) ("Google Decision") (collecting cases and granting search warrant application requiring Internet service provider to turn over all email communications for a specific period that would be reviewed by the government off-site).

The two-step approach to executing an email search warrant, in which the Internet service provider discloses to the government all emails related to an individual's email account specified in Attachment A, and the government then reviews those emails to determine whether they fall within Attachment B, is reasonable and not overbroad. In approving a search warrant of a computer hard drive, the Third Circuit recently held that hard drives collected during the

execution of a search warrant did not have to be searched "on-site" because the "practical realities of computer investigations preclude on-site searches." United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011). The court further explained that "as a practical matter, '[w]hen a search requires review of a large collection of items, such as papers, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."'" Id. at 234 (quoting United States v. Williams, 592 F.3d 511, 519-20 (4th Cir. 2010) (in turn quoting Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976))). Indeed, every court of appeals to consider the issue has endorsed the two-step process for warrants seeking electronic evidence. See, e.g., United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012) (explaining that "[t]he federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer haystack") (citations and internal quotation marks omitted); United States v. Grimmett, 439 F.3d 1263, 1268–70 (10th Cir. 2006); United States v. Hay, 231 F.3d 630, 637-38 (9th Cir. 2000); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).[2]

Similarly, the Eighth Circuit upheld as reasonable the execution of a two-step warrant for email stored with a web-based email provider in United States v. Bach, 310 F.3d 1063, 1067-68 (8th Cir. 2002). In Bach, an investigator "obtained a state search warrant to retrieve from

[2] Appellate courts have also approved off-site sorting in cases involving paper documents, rather than electronic evidence. See, e.g., United States v. Santarelli, 778 F.2d 609, 616 (11th Cir. 1985) (upholding off-site examination of documents from defendant's desk and four-drawer filing cabinet); United States v Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (upholding seizure of an entire file cabinet because seizure was motivated by the impracticability of on-site sorting).

Yahoo! e-mails between the defendant and possible victims of criminal sexual conduct, as well as the Internet Protocol addresses connected to his account." Id. at 1065. However, Yahoo! employees did not attempt to find this particular information:

> Yahoo! technicians retrieved all of the information from Bach's account at dlbch15@yahoo.com and AM's Yahoo! e-mail account. According to Yahoo!, when executing warrants, technicians do not selectively choose or review the contents of the named account. The information retrieved from Bach and AM's accounts was either loaded onto a zip disc or printed and sent to [a law enforcement officer]. E-mails recovered from Bach's account detail him exchanging pictures with other boys and meeting with them.

Id. The court upheld this search as reasonable under the Fourth Amendment. Id. at 1067-68.

The procedures used to execute the warrant in Bach have also been upheld by the majority of district courts to consider the issue. See, e.g., United States v. Lee, No. 1:14-cr-227-TCB-2, 2015 WL 5667102, at *3 (N.D. Ga. Sept. 25, 2015) ("[I]n the Court's view, the weight of the authority supports the conclusion that a warrant that requires disclosure of the entire contents of an email account and then describes a subset of that information that will be subject to seizure is reasonable."); United States v. Pugh, No. 1:15-CR-00116-NGG, 2015 WL 9450598, at *27 (E.D.N.Y. Dec. 21, 2015); United States v. Scully, No. 14-CR-208 (ADS) (SIL), 2015 WL 3540466, at *31-34 (E.D.N.Y. June 8, 2015); United States v. Ulbricht, No. 14-CR-68 (KBF), 2014 WL 5090039, at *15 (S.D.N.Y. Oct. 10, 2014); Matter of Search of Info. Associated with [redacted]@ mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 164 (D.D.C. 2014); Google Decision, 33 F. Supp. 3d at 394; United States v. Ayache, No. 3:13-cr-153 (AAT), 2014 WL 923340, at *2-3 (M.D. Tenn. Mar. 10, 2014); United States v. Deppish, 994 F. Supp. 2d 1211, 1219-20 & n.37 (D. Kan. 2014); United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011); United States v. Bowen, 689 F. Supp. 2d 675,

682-85 (S.D.N.Y. 2010); United States v. McDarrah, No. 05-cr-1182 (PAC), 2006 WL 1997638, at *9-10 (S.D.N.Y. July 17, 2006), aff'd, 351 F. App'x 558 (2d Cir. 2009).[3]

Amendments to Federal Rule of Criminal Procedure 41 enacted in 2009, moreover, explicitly adopt this two-step procedure. See Fed. R. Crim. P. 41, Advisory Committee's Notes (2009 amend.). The amendments were promulgated by the Supreme Court. See 28 U.S.C. § 2072. Rule 41 now provides that a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B).

Here, the Email Search Warrants followed the two-step procedure explicitly authorized by Stabile and Rule 41: the government received electronic documents within the scope of Attachment A from the Internet service provider, which the government then reviewed to identify and seize the more limited set of documents that constitute evidence of crimes within the scope of Attachment B. See Stabile, 633 F.3d at 234. Thus, the warrants are not overbroad because the Internet service providers disclosed "all email communications" for the relevant email addresses, as the defendant contends. (Br. at 16 (emphasis omitted).) That disclosure was proper under Stabile because agents are constrained by Attachment B in identifying and seizing

[3] The two out-of-circuit district court cases on which the defendant relies are contrary to the Third Circuit's decision in Stabile and the weight of authority. (Br. at 12-13 (citing In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013) and In the Matter of the Search of Google Email Accounts Identified in Attachment A, 92 F. Supp. 3d 944, 953 (D. Alaska 2015)).)

evidence of enumerated crimes in documents created after February 1, 2007.[4] Accordingly, the Email Search Warrants were not overbroad.

C. The Email Search Warrants Were Amply Supported by Probable Cause

The Email Search Warrants authorized the seizure of items for which there was ample probable cause. The Gray Affidavit described in detail evidence establishing probable cause that the defendant participated in a complex bribery scheme and that evidence of those crimes would be found in the Chestnut Email Account and the Gmail Email Account.

"The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). "That determination does not require absolute certainty that evidence of criminal activity will be found at a particular place, but rather that it is reasonable to assume that a search will uncover such evidence." Yusuf, 461 F.3d at 390 (citing United States v. Ritter, 416 F.3d 256, 263 (3d Cir. 2005)). Probable cause determinations must be approached in a practical way, Gates, 462 U.S. at 231-32, because "probable cause is a flexible, common-sense standard." Texas v. Brown, 460 U.S. 730, 742 (1983). "The probable cause determination is to be made only after considering the totality of the circumstances, which requires courts to consider the cumulative weight of the information set forth by the investigating officer in connection with reasonable inferences that the officer is permitted to make based upon the officer's specialized

[4] The defendant wrongly contends that "the warrant affidavit cannot be employed to limit the searches here because the affidavit was sealed and did not accompany the warrants served on the service providers." (Br. at 17.) Because the Internet service providers simply disclosed the contents of the email accounts, which were later reviewed for relevance off-site by the government, it was unnecessary for the Internet service providers to receive a copy of the Gray Affidavit. Attachment B to each warrant, moreover, more than sufficiently constrains the agents reviewing the produced emails.

training and experiences." Yusuf, 461 F.3d at 390 (citing United States v. Arvizu, 534 U.S. 266, 275 (2002)).

Once a neutral and detached magistrate issues a search warrant upon a finding of probable cause, that finding is subject to "great deference by reviewing courts." United States v. Conley, 4 F.3d 1200, 1205 (3d Cir. 1993) (emphasis in original) (citations and internal quotation marks omitted). The duty of a court reviewing a magistrate judge's probable cause determination is "simply to ensure that the magistrate had a substantial basis for . . . conclud[ing] that probable cause existed." Gates, 462 U.S. at 238 (quoting Jones v. United States, 362 U.S. 257, 271 (1960)) (alterations in original). "[A] reviewing court may not conduct a de novo review of a probable cause determination," and must "uphold a warrant so long as the issuing magistrate's determination was made consistent with the minimal substantial basis standard." Conley, 4 F.3d at 1205 (citing Gates, 462 U.S. at 236).

The Gray Affidavit recounted numerous specific facts establishing probable cause that the defendant had participated in a criminal bribery scheme and that evidence of his crimes would be found in his email accounts. These facts included: (i) a whistleblower report that the defendant bribed an EBRD official (Gray Aff. ¶ 6); (ii) banking records reflecting payments from the defendant's company to the EBRD official's sister (id. ¶¶ 7-9); (iii) contracts between the defendant's company and its clients awarding substantial "success fee[s]" to the defendant's company for securing EBRD contracts (id. ¶ 38); (iv) testimony from interviews revealing that neither the defendant's company nor the EBRD official's sister provided any services in connection with negotiating the EBRD contracts (id. ¶¶ 49-52); (v) an EBRD official report that the defendant participated in a scheme to bribe the EBRD official (id. ¶ 57); and (vi) numerous summaries and excerpts of emails sent to and from the Chestnut Email Account and the Gmail

Email Account revealing that the defendant used the accounts to discuss, among other things, payments to the EBRD official's sister and the projects that the defendant secured for his clients by making bribe payments to the EBRD official through his sister (id. ¶¶ 60, 66).

The defendant argues that two of the specific categories of communications that Attachment B to each warrant permits the government to seize are overbroad and not supported by probable cause. He contends, wrongly, that the warrants permit the government to seize "all communications between Mr. Harder 'and employees of Chestnut Consulting Group, Inc.' as well as all communications between Mr. Harder 'and financial institutions at which the Subjects banked during the course of the scheme.'" (Br. at 17.) The warrants do not permit such a broad seizure. Instead, they permit the government to seize documents falling within the seven categories of documents identified in each Attachment B only when those documents (i) "constitute[] the fruits, evidence, and instrumentalities of violations" of specific enumerated crimes; and (ii) "involve[e] Dmitrij Harder, Andrey Ryjenko, Tatjana Sanderson ("Subjects") since February 1, 2007 . . . ." (Br. Attach. A. at 38-39, Attach. B. at 38-39.) The Gray Affidavit supporting the applications for the Email Search Warrants more than amply establishes probable cause for such circumscribed seizures.[5]

D. The Gray Affidavit Does Not Include Illegally-Obtained Information

The defendant separately argues that the Email Search Warrants should be suppressed because they rely for probable cause on statements he made during his February 26, 2010, interview at JFK, and because "[m]ore importantly, it was during that interrogation when Mr. Harder provided the name of the Chestnut Consulting email account, which was the subject of

[5] Should the Court find the probable cause established by the Gray Affidavit in some manner deficient, the executing agents plainly had an objectively reasonable reliance on the warrant's authority. See United States v. Leon, 468 U.S. 897 (1984); United States v. Hodge, 246 F.3d 301, 305 (3d Cir. 2001).

the search warrant directed to 1&1 Internet." (Br. at 18.) Those arguments fail for four reasons. First, the defendant's statements during the JFK interview were voluntary and should not be suppressed, for the reasons the government has previously submitted to the Court. (Doc. Nos. 56, 75, 96.) Second, even if the Court omitted the defendant's false exculpatory statements during the February 26, 2010, interview recounted in the Gray Affidavit, the affidavit would still amply establish probable cause for both of the defendant's email accounts. Third, as the Gray Affidavit makes clear, the government learned of the defendant's email account hosted by 1&1 Internet from both the defendant's subpoena returns and from the EBRD and City of London Police. (Gray Aff. ¶¶ 44, 52, 62, 63, 70.) Thus, even had the defendant not provided a single document in response to the subpoenas served on him, the government would still have discovered the 1&1 Internet email account and the relevant emails from it to Ryjenko recounted in the Gray Affidavit. And, fourth and finally, the defendant has never moved to suppress the documents he provided in response to the subpoenas. Nor could he do so, as the subpoenas are plainly not the fruit of the (in any case constitutional) JFK interview.

E. The Email Search Warrants Were Not Required to Include Search Protocols

The defendant is correct that Email Search Warrants do not include a search protocol or protocols to "to segregate, seal, and/or return material that is irrelevant and not supported by probable cause, or privileged." (Br. at 18.) Most courts have found, however, that email search warrants are not required to have such protocols.

According to the Supreme Court, "[n]othing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed." United States v. Grubbs, 547 U.S. 90, 98 (2006) (quoting Dalia v. United States, 441 U.S. 238, 255 (1979)). "Not surprisingly, in the context of computer searches, such direction is routinely held not to be

required." Google Decision, 33 F. Supp. 3d at 399 (collecting cases). The Sixth Circuit has explained that "given the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis." United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011).

Courts considering search warrant applications related to email accounts have refrained from requiring the government to undertake particular search methods or adopt specified document filters. See Google Decision, 33 F. Supp. 3d at 400 ("To limit the government's computer search methodology ex ante would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents or other creative data concealment techniques . . . . Our inability to predict the best mechanism for conducting a search strongly counsels against including any search protocol in a warrant." (citations and quotation marks omitted)); Deppish, 994 F. Supp. 2d at 1220 ("[N]othing in § 2703 precludes the Government from requesting the full content of a specified email account, nor has the Tenth Circuit ever required warrants to identify a particularized search strategy." (citation omitted)); Taylor, 764 F. Supp. 2d at 237 ("The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching." (citation omitted)).

The defendant has asserted that the mere fact that the warrant returns may have contained privileged material renders them for some reason invalid. Tellingly, the defendant does not cite a single case where a court suppressed evidence obtained pursuant to an otherwise valid warrant

because it did not include a search protocol for relevance and privileged documents. The government has appropriately segregated potentially privileged material and set up a separate filter team to review them. Further, even if—contrary to fact—a member of the prosecution team had inadvertently reviewed privileged material, the appropriate remedy would not be suppression.

The defendant also contends that all information received in response to the Email Search Warrants should be suppressed because the warrants did not include a protocol requiring that the government either segregate, return, or destroy information found to be outside the scope of the warrants by a certain deadline. The defendant is wrong. "[T]he Government has a need to retain materials as an investigation unfolds for the purpose of retrieving material that is authorized by the warrant." Google Decision, 33 F. Supp. 3d at 398. It is also "necessary for the Government to maintain a complete copy of the electronic information to authenticate evidence responsive to the warrant for purposes of trial." Id. at 399. Moreover, as noted above, warrant protocols of the type advocated by the defendant are generally disfavored.

The defendant's reliance on the Second Circuit's decision in United States v. Ganias is misplaced. (Br. at 21-22 (citing 755 F.3d 125 (2d Cir. 2014), reh'g en banc granted, 791 F.3d 290 (2d Cir. 2015)).) There, the government secured a warrant for information related to accounting services the defendant had provided to two companies. Id. at 128. During the search, the government seized the defendant's personal records—which were beyond the scope of the warrant—and kept the records for two-and-a-half years before developing probable cause to believe they contained evidence that he had committed a different crime. Id. at 128–29. The Second Circuit held the government violated the defendant's Fourth Amendment rights by retaining the records for an unreasonable amount of time and seeking to use them in an unrelated

criminal investigation. Id. at 137. Here, the government is not using the records as a basis for an unrelated criminal investigation not authorized by the warrant and is holding the search warrant returns for appropriate reasons, including authentication.

III. The Email Search Warrants Complied with Rule 41 of the Federal Rules of Criminal Procedure

A. The Government Had No Obligation to Notify the Defendant of the Email Search Warrants

The government was not, contrary to the defendant's assertion, required to notify him of the issuance and execution of the Email Search Warrants. In United States v. Bansal, the defendant made an identical argument—that the government failed to notify him in connection with the execution of an email search warrant on an Internet service provider. 663 F.3d 634, 662 (3rd Cir. 2011). The Third Circuit affirmed this Court's denial of the defendant's motion to suppress and held that because "[t]he plain text of Rule 41 . . . requires notice only 'to the person from whom, or from whose premises, the property was taken,'" it was only necessary to provide notice "to the internet service providers upon whom the search warrants were executed." Id. (emphasis in original). Here, the defendant does not deny that the government provided the warrant to Google and 1&1 Internet. Nor are Internet service providers required to provide notice to their users when the government has executed a search warrant.

B. The Magistrate Judge Was Authorized to Issue the Google Search Warrant

Finally, the defendant argues that Judge Restrepo was not authorized to issue a search warrant directed to Google because Google is located in California and thus outside the Eastern District of Pennsylvania. The Third Circuit, however, rejected this precise argument in Bansal. There, five magistrate judges in this District issued warrants for emails executed upon Google and MSN Hotmail, both of which are in California. Affirming this Court, the Third Circuit

rejected the very argument advanced by the defendant here—that Rule 41 controls and limits a magistrate judge's jurisdiction:

> The procedures that federal and state law enforcement officers must follow when compelling disclosure from network service providers is set forth at 18 U.S.C. § 2703(a). The version of the statute in effect when these warrants were issued in 2004 authorized any "court with jurisdiction over the offense under investigation" to issue a warrant for electronic communications—even if the warrants were ultimately executed in another state. See § 2703(a). Bansal contends that Rule 41(b), which limits a Magistrate Judge's jurisdiction to the District in which he or she sits, trumps § 2703(a). We, along with other courts to consider the question, reject that contention.

Bansal, 663 F.3d at 662 (citing United States v. Berkos, 543 F.3d 392, 396-98 (7th Cir. 2008) (holding that Rule 41(b) "does not apply to § 2703(a)")). The defendant neither discusses this controlling Third Circuit decision nor cites a single decision supporting his position.[6] Section 2703(a) of Title 18, moreover, permits a "court of competent jurisdiction" to issue an email search warrant. A "court of competent jurisdiction" includes "any district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated . . . ." 18 U.S.C. § 2711(3)(A)(i). Accordingly, Judge Restrepo was authorized to issue the Email Search Warrants.

[6] The defendant does, however, identify a district court decision from the Eastern District of New York which, like the Third Circuit in Bansal, held that 18 U.S.C. § 2703(a) "authorizes electronic search warrants by a federal magistrate judge that extend outside his or her district." United States v. Scully, 108 F. Supp. 3d 59, 83 (E.D.N.Y. 2015). (Br. at 24.)

CONCLUSION

For the reasons set forth above, the government respectfully requests that the Court deny the defendant's motion to suppress electronic evidence obtained from Google and 1&1 Internet in connection with the Email Search Warrants.

Respectfully submitted,

ZANE DAVID MEMEGER
UNITED STATES ATTORNEY

/s/ Michelle L. Morgan
MICHELLE L. MORGAN
Assistant United States Attorney

ANDREW WEISSMANN
Chief, Fraud Section
Criminal Division, U.S. Department of Justice

/s/ Jason D. Linder
JASON D. LINDER
Senior Trial Attorney, Fraud Section
Criminal Division, U.S. Department of Justice

CERTIFICATE OF SERVICE

I certify that on this day I caused a copy of the government's response in opposition to the defendant's motion to suppress to be served by ECF filing on:

Stephen R. LaCheen
1429 Walnut Street, 13th Floor
Philadelphia, PA 19102 US

Ian Comisky, Esq.
Blank Rome LLP
One Logan Square
Philadelphia, PA 19103

/s/ Michelle L. Morgan
MICHELLE L. MORGAN
Assistant United States Attorney

Date: March 16, 2016